

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with IP address
108.167.180.224 that is stored at premises owned,
maintained, controlled, or operated by Endurance
International Group, Inc., a company headquartered
at 10 Corporate Drive, Suite 300, Burlington, MA

Case No. 16M123

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

over which the Court has jurisdiction pursuant to Title 18, United States Code, Sections 2703 and 2711, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of:
18 U.S.C. §§ 1030, 1341, and 371

The application is based on these facts: See attached affidavit.

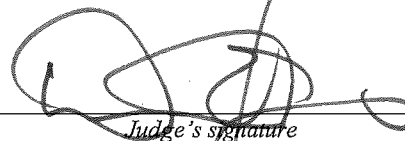
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

FBI Special Agent Jill Dring
Printed Name and Title

Sworn to before me and signed in my presence:

Date: Oct 7, 2016


Judge's signature

AFFIDAVIT

I, Jill A. Dring, being duly sworn and under oath state the following:

Introduction and Agent Background

1. I am a Special Agent with the Federal Bureau of Investigation. I have been employed with the FBI since May of 2012. I am currently assigned to the FBI Milwaukee Division's Cyber Crimes Task Force.

2. As a Special Agent with the FBI, I investigate criminal and national security related computer intrusion matters involving botnets, distributed denial of service attacks, the distribution of SPAM, malicious software, the theft of personal identifying information, and other computer-based fraud. Since joining the FBI, I have been involved in numerous criminal and national security investigations involving computer intrusions. I have received training in computer technology and computer-based fraud.

3. This affidavit is made in support of an application for a warrant under 18 U.S.C. §§ 2703(a), (b)(1)(A) and (c)(1)(A) and Federal Rule of Criminal Procedure 41 to require Endurance International Group ("EIG"), located at 10 Corporate Drive, Suite 300, Burlington, MA 01803, to disclose to the United States copies of the information related to violations of 18 U.S.C. §§ 1030(a)(5)(A), 1343, and 371, as further described in Attachment B, stored at premises owned, maintained, controlled, or operated by EIG, as further described in Attachment A.

4. The statements in this affidavit are based on my personal knowledge, and information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of an application for a search warrant, I have

not included every fact known to me concerning this investigation. Instead, I have only set forth facts that I believe are necessary to establish probable cause for the issuance of a warrant.

5. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 1030(a)(5)(A), 1343, and 371 (the “Subject Offenses”) have been committed; and fruits, evidence, and instrumentalities of those violations, as further described in Attachment B will be found in the information associated with IP address **108.167.180.224** is located at a facility owned or controlled by EIG as further described in Attachment A.

Jurisdiction to Issue the Warrant

6. EIG is a “remote computing service” as defined by 18 U.S.C. § 2711(2), and is therefore subject to the provisions of 18 U.S.C. § 2703.

7. According to 18 U.S.C. § 2703(a), (b)(1)(A) & (c)(1)(A) “court of competent jurisdiction” may issue warrants that require a “remote computing service” to disclose certain subscriber and customer records and electronic communications.

8. A “court of competent jurisdiction” is “any district court of the United states (including a magistrate judge of such a court) or any United States court of appeals that – (i) has jurisdiction over the offense being investigated” This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

Background Information on Web Hosting Companies

9. Web hosting companies, such as EIG, maintain server computers connected to the Internet. Their customers typically use those computers to operate websites on the Internet.

10. In general, web hosting companies like EIG ask each of their customers to provide certain personal identifying information when registering for an account. This information can include the customer's full name, physical address, telephone number and other identifiers, e-mail addresses, and business information. Web hosting companies also may retain records of the length of service (including start date) and types of services utilized. In addition, for paying customers, web hosting companies typically retain information about the customers' means and source of payment for services (including any credit card or bank account number).

11. Web hosting companies like EIG allow customers to place files, software code, databases, and other data on the servers. To do this, customers connect from their own computers to the server computers across the Internet.¹ This connection can occur in several ways. In some situations, it is possible for a customer to upload files using a special web site interface offered by the web hosting company. It is frequently also possible for the customer to access the server computer directly through the Secure Shell ("SSH") or Telnet protocols. These protocols allow remote users to type commands to the web server. The SSH protocol can also be used to copy files to the server. Customers can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet, and FTP connections, showing the dates and times of the connections, the method of connecting, and the Internet Protocol addresses ("IP addresses") of the remote users' computers (IP addresses are used to identify computers connected to the Internet). Servers also commonly log the port

¹ In this case, as described below, unidentified individuals are connecting to a EIG server (identified by IP address **108.167.180.224**); and they are using the server to facilitate violations of the Subject Offenses.

number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.

12. The servers use those files, software code, databases, and other data to respond to requests from Internet users for pages or other resources from the website. Commonly used terms to describe types of files sent by a server include HyperText Markup Language (“HTML”) (a markup language for web content), Cascading Style Sheets (“CSS”) (a language for styling web content), JavaScript (a programming language for code run on the client’s browser), and image files. Web hosting companies frequently allow their customers to store collections of data in databases. Software running on the web server maintains those databases; two common such programs are named MySQL and PostgreSQL, although these are not the only ones.

13. Web sites deliver their content to users through the Hypertext Transfer Protocol (“HTTP”). Every request for a page, image file, or other resource is made through an HTTP request between the client and the server. The server sometimes keeps a log of all of these HTTP requests that shows the client’s IP address, the file or resource requested, the date and time of the request, and other related information, such as the type of Web browser the client uses.

Facts Supporting Probable Cause²

14. Since approximately January 2015, the FBI Milwaukee Division’s Cyber Crimes Task Force has been investigating a data breach involving the use of information stealing malware at a healthcare provider (“HCP”) located in the Eastern District of Wisconsin. Based on the investigation to date, the malware, known by the name “Qakbot” or “Qbot,” is being used

² In this affidavit, unless otherwise noted, an IP address represents a server or computer which is identifiable by or associated with the listed IP address.

to steal personal identifying information (“PII”) and financial-related information associated with banking activity conducted over compromised computer networks.

15. In January 2015, the FBI received information from a HCP located in the Eastern District of Wisconsin that it had identified suspicious activity on its computer network. An employee at the HCP determined that the HCP’s computer network had been compromised with information-stealing malware. The HCP informed the FBI that it determined that approximately 800 computers operating on its computer network were compromised with the malware.

16. The HCP provided an image of one of the compromised HCP servers to the FBI for analysis. A computer scientist at the FBI examined the functionality of the malware found on the HCP server and determined the malware to be a variant of the Qbot malware. Based on an analysis of the malware, the FBI determined that the malware damaged each computer it compromised because it modified existing programs on the compromised computer and installed new programs on the compromised computer.

17. According to the FBI analysis of the Qbot malware, the modified and newly installed programs caused a compromised computer³ to execute a series of unauthorized commands that collected and transferred PII and banking information from the compromised computer to a server identified in the malware. For example, the FBI analysis of the malware showed that the malware functioned as a keystroke logger and recorded the usernames and passwords used to access banking and financial websites through a compromised computer. Any usernames and passwords recorded by the keystroke logger were encrypted and transferred (at the time) to IP address 173.254.28.15 (and domain nickspizzade.com) used by a by a pizzeria located in the U.S. PII and other information collected by the malware were transferred to

³ As used in this affidavit, a “compromised” or “infected” computer is a computer system on which Qbot has been installed.

another set of servers located in the U.S. At the time of the FBI analysis, a finite number of IP addresses were coded into the malware and were utilized to receive the encrypted information.

18. On or about August 6, 2015, U.S. Magistrate Judge Nancy Joseph authorized the installation and use of a pen register and trap and trace device or process ("pen-trap device") to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from IP address 173.254.28.15 associated with the domain name nickspizzade.com. Results from the pen-trap device on that IP address showed communications between IP address 173.254.28.15 and IP addresses (based on publicly available information through centralops.net)⁴ located in multiple foreign countries, including: Australia, Austria, Belgium, Brazil, Bulgaria, Canada, China, Colombia, Egypt, France, Germany, Guyana, Hungary, Indonesia, Israel, Italy, Korea, Lithuania, Mozambique, the Netherlands, New Zealand, Pakistan, Poland, and Russia. Based on my experience and familiarity with this investigation, and information obtained from other experienced individuals, I believe those communications represented the transfer of stolen information from a compromised computer to IP address 173.254.28.15.

19. As of January 17, 2016, one server coded into the malware was IP address 69.195.124.60, which resolved to a U.S.-based server operated by host company named Blue Host.⁵ The FBI obtained IP login data for IP address 69.195.124.60 from Blue Host. That IP login data listed the IP addresses that accessed IP address 69.195.124.60 between January 17,

⁴ Centralops.net is publicly available website that lists contact and registry information for domain names and IP addresses.

⁵ It appeared that malware receives regular updates through various servers. The updates allowed the attackers to modify the malware based on actions taken to mitigate the exfiltration of stolen PII and banking credentials. Because of the malware is updated on a regular basis, the FBI analysis of the malware is ongoing.

2016 and February 4, 2016. Analysis of the data logs showed that encrypted files had been transferred to IP address 69.195.124.60. And the data logs showed that those encrypted files were download from IP address 69.195.124.60, and then deleted from IP address 69.195.124.60 by an unidentified individual(s) utilizing the IP addresses that were owned and controlled by service providers located in Germany and the Netherlands.⁶

20. According to the owner of IP address 69.195.124.60 (Blue Host), the above-described activity on IP address 69.195.124.60 was unauthorized. Based on my experience and familiarity with the investigation, and information obtained from other experienced individuals, I believe the encrypted files transferred, downloaded, and deleted from IP address 69.195.124.60 contained stolen financial login credentials and/or stolen PII obtained from computers infected with Qbot. Using data logs from Blue Host, the FBI identified IP addresses responsible for transferring the encrypted files to IP address 69.195.124.60. Based on my experience and familiarity with the investigation, and information obtained from other experienced individuals, I believe each IP address represented a computer infected with Qbot. Based on publicly available information for each IP address, the compromised computers were located around the world. The FBI identified approximately 500 unique IP addresses that resolve to locations in the U.S.

21. On or about January 24, 2016, through the United States Computer Emergency Readiness Team ("US-CERT"), the FBI learned of two additional HPCs compromised with Qbot. According to US-CERT, one of those newly identified HCPs was located in Massachusetts, and the other HCP was located in Melbourne, Australia.

⁶ This was determined using publically available registry information for those IP addresses.

22. The HCP located in Melbourne hired BAE Systems ("BAE") to mitigate the impact of the malware on their computer network.⁷ Affiant communicated with representatives from BAE, on multiple occasions during this investigation. According to a representative from BAE, they analyzed the malware found at the Melbourne HCP and found five specific domain names written into the malware. Based on my experience and familiarity with the investigation, and information obtained from other experienced individuals, I believe those domains were being used by the attackers to exfiltrate stolen PII and banking information from compromised computer systems.

23. Affiant obtained the list of domain names from BAE, and searched publicly available domain registration information for the domain names using centralops.net. According to information obtained from centralops.net, the domain names found in the Melbourne HCP data breach resolved to IP addresses 69.195.124.60; 50.87.150.203; 181.224.138.240; 173.254.28.15; and 162.144.12.241, which were owned by U.S.-based companies Blue Host, Site Ground, Just Host, and HostGator.

24. The FBI obtained an image of an compromised computer from the HCP located in Massachusetts. A computer scientist at the FBI examined the functionality of the malware found on the compromised computer. The FBI analysis found that the same the same five domains from the Melbourne HCP infection were listed in the malware sample from Massachusetts HCP. Those domains also resolved to IP addresses 69.195.124.60; 50.87.150.203; 181.224.138.240; 173.254.28.15; and 162.144.12.241.

⁷ According to their web site, BAE is a global defense, aerospace and security company employing approximately 83,400 people worldwide. BAE Systems has not been compensated for any information it provided to the FBI related to this investigation.

25. On February 25, 2016, U.S. Magistrate Judge Nancy Joseph issued search warrants authorizing the search and seizure of information associated with IP addresses 69.195.124.60; 50.87.150.203; 181.224.138.240; 173.254.28.15; and 162.144.12.241. The search warrants were served on host companies Blue Host, Site Ground, Just Host, and HostGator a short time later. Based on an analysis of the information obtained through the search warrants and other information obtained during the course of the investigation, the FBI determined that the servers associated with those IP addresses were accessed without authorization; and that during the unauthorized access, and encrypted files that had been transferred to the servers from victimized computer networks were downloaded and then deleted. The FBI also identified user names and passwords for various accounts in the files being transferred to and from those servers. Based on my involvement in this investigation and the types of accounts associated with those usernames and passwords, I believe those usernames and passwords were transferred without authorization to the server on which it was located, from a computer infected with Qbot.

26. On or about April 6, 2016, a researcher from Intel Security (“Intel”) provided information to the FBI regarding servers being utilized by Qbot at that time.⁸ According to the researcher, Intel was studying the functionality of Qbot, which it referred to as the “pinkslip bot.” According to the researcher at Intel, based on his review of the Qbot malware, the following servers were coded into the version of Qbot in use at that time:

```
ftphost_1=66.96.133.9:help  
ftphost_2=196.12.12.88:log@zica.co.zm  
ftphost_3=91.199.120.147:logs@ixl030cf.ixl.es  
ftphost_4=50.87.114.63:cpanel@itsolution-lb.com
```

⁸ Intel is subsidiary of the Intel Corporation. According to publicly available information, Intel is a global network and software security company that is based in the U.S. Intel has not been compensated for any information it provided to the FBI related to this investigation.

27. On April 19, U.S. Magistrate Judge David E. Jones issued search warrants authorizing the search and seizure of information associated with IP addresses 66.96.133.9 and 50.87.114.63, which were two of the IP addresses identified by Intel.

28. The search warrants were served and executed a short time later. Based on an analysis of the information obtained through the search warrants and other information obtained during the course of the investigation, the FBI determined that the servers associated with the IP addresses listed in paragraph 23 were accessed without authorization; and that during the unauthorized access, encrypted zip files that had been transferred to those servers from a victimized computer network were downloaded and then deleted. The FBI also identified user names and passwords for various accounts in the files being transferred to and from those servers. Based on my involvement in this investigation and the types of accounts associated with those usernames and passwords, I believe those usernames and passwords were transferred without authorization from a computer compromised with Qbot to the server on which it was located.

29. On or about May 16, 2016, a representative from Intel informed the FBI that through its analysis of the most up-to-date version of Qbot (at that time), Intel had identified an encrypted DLL⁹ file coded into the malware.¹⁰ According to the representative from Intel, they successfully decrypted the DLL file and determined the DLL contained, among other things, a JavaScript program that included a list of domain names from which an infected computer attempted to download the most current version of the Qbot malware every 15 hours. One of those listed domains was engine.perksautocare.com, which resolved to **108.167.180.224**. Intel

⁹ A dynamic-link library (DLL) file is an executable file that allows programs to share code and other resources necessary to perform particular tasks.

¹⁰ According to a FBI computer scientist, the DLL file is installed on the compromised computer and remains on the compromised computer until the computer is rebooted.

tested the functionality of the domains listed in the JavaScript program and determined that each domain is the functional equivalent of a command and control server. Based on my training and experience and information obtained from other experienced agents, I know (as it relates to this investigation) a command and control server is a computer used by an individual to issue commands to a computer infected with the Qbot malware and control its operation without the owner's authorization.

30. According to information obtained from centralops.net, **108.167.180.224** registered with the web hosting business Websitewelcome.com. Based on information obtained from a EIG, EIG does business as Websitewelcome.com, and possesses information associated with **108.167.180.224**.

31. On or about June 13, 2016, U.S. Magistrate Judge William E. Duffin authorized the installation and use of a pen-trap device on IP address **108.167.180.224**. I have reviewed the pen-trap data for IP address **108.167.180.224** and analyzed the traffic for remote logins to that computer system. The results showed communications between IP address **108.167.180.224** and IP addresses located in China, the Czech Republic, Germany, France, the Netherlands, Russia, and the Ukraine, among other countries.¹¹ Based on my training and experience, and information from other experienced individuals, and the preceding information in the preceding paragraphs, I believe the server associated with IP address **108.167.180.224** is being accessed without authorization; and is being used as a command and control sever to issue commands to a computer compromised with the Qbot malware and control its operation without the owner's authorization.

¹¹ The location of the other IP addresses was determined using publically available registry information for those IP addresses.

32. On or about September 6, 2016, a preservation letter pursuant to 18 U.S.C. § 2703(f) was issued to EIG in order to preserve information located on the server associated with IP address **108.167.180.224**.

Information to be Searched and Things to be Seized

33. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), and Federal Rule of Criminal Procedure 41 by using the warrant to require EIG to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

Conclusion

34. Based on the information stated above, I respectfully submit that probable cause exists to believe that violations of the Subject Offenses have been committed and fruits, evidence, instrumentalities concerning those violations, as further described in Attachment B will be located on the servers associated with IP address **108.167.180.224**, as further described in Attachment A.

35. Because the warrant will be served on EIG who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with IP addresses **108.167.180.224** that is stored at premises owned, maintained, controlled, or operated by Endurance International Group, 10 Corporate Drive, Suite 300, Burlington, MA 01803.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Endurance International Group (“EIG”)

To the extent that the information described in Attachment A is within the possession, custody, or control of EIG, including any messages, records, files, logs, or information that have been deleted but are still available to EIG, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), EIG is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. all records or other information pertaining to the customers of IP address **108.167.180.224**, including all files, databases, and database records stored by EIG in relation to customers of IP address **108.167.180.224**;

b. all information in the possession of EIG that might identify the subscribers related to those accounts or identifiers, including names, addresses, telephone numbers and other identifiers, e-mail addresses, business information, the length of service (including start date), means and source of payment for services (including any credit card or bank account number), and information about any domain name registration; and

c. all records related to network traffic on the server associated with IP addresses **108.167.180.224**, including records of remote logins.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1030, 1341, and 371, involving unknown individuals since at least May 16, 2016, relating to the development, access, use, administration

or maintenance of **108.167.180.224** for maintain the Qbot malware and accessing computer compromised with the Qbot malware, including:

1. files, databases, and database records stored by EIG on behalf of the subscriber or user of IP address **108.167.180.224**, including:

- a. programming code used to serve or process requests made via web browsers;
- b. HTML, CSS, JavaScript, image files, or other files;
- c. HTTP request and error logs; and
- d. SSH, FTP, or Telnet logs showing connections related to the website, and any other transactional information, including records of session times and durations, log files, encrypted .zip files, dates and times of connecting, methods of connecting, and ports.